116TH CONGRESS
2d Session
HOUSE OF REPRESENTATIVES
REPT. 116–683
Part 1

NATIONAL COMMISSION ON ONLINE PLATFORMS AND HOMELAND SECURITY ACT

DECEMBER 21, 2020.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Mr. THOMPSON of Mississippi, from the Committee on Homeland Security, submitted the following

R E P O R T

together with

MINORITY VIEWS

[To accompany H.R. 4782]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security, to whom was referred the bill (H.R. 4782) to establish a national commission on online platforms and homeland security, and for other purposes, having considered the same, reports favorably thereon with an amendment and recommends that the bill as amended do pass.

CONTENTS

19–006

The amendment is as follows:

Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the "National Commission on Online Platforms and Homeland Security Act".

SEC. 2. NATIONAL COMMISSION ON ONLINE PLATFORMS AND HOMELAND SECURITY.

(a) ESTABLISHMENT OF COMMISSION.—There is established a National Commission on Online Platforms and Homeland Security (referred to in this section as the "Commission").

(b) PURPOSES.—The Commission shall—

(1) identify, examine, and report on the ways, if any, that online platforms have been utilized in furtherance of acts of targeted violence, including domestic terrorism and international terrorism, or covert foreign state influence campaigns; and

(2) identify, examine, and report on the ways, if any, that free speech, privacy, civil rights, and civil liberties are impacted by—

(A) any utilization of online platforms in furtherance of acts of targeted violence, including domestic terrorism and international terrorism, or covert foreign state influence campaigns; and

(B) any policies, procedures, or activities undertaken by owners and operators of online platforms to prevent or limit the utilization of online platforms in furtherance of acts of targeted violence, including domestic terrorism and international terrorism, or covert foreign state influence campaigns; and

(3) develop recommendations, as appropriate, for how online platforms could address the utilization identified pursuant to paragraph (1), if any, in ways that are transparent and accountable, to promote free speech and innovation on the internet, preserve individual privacy, civil rights, and civil liberties, and uphold the principles of the Constitution, in accordance with relevant existing statutes, including section 552a of title 5, United States Code (commonly referred to as the Privacy Act of 1974), and take into account current or anticipated trends and technological developments, such as advancements in artificial intelligence.

(c) COMPOSITION OF COMMISSION.—

(1) MEMBERS.—The Commission shall be composed of 12 members, of whom—

(A) two members shall be appointed by the Committee on Homeland Security in the House of Representatives, with one member selected by the Chair and the other selected by the Ranking Member;

(B) two members shall be appointed by the Committee on Foreign Affairs in the House of Representatives, with one member selected by the Chair and the other selected by the Ranking Member;

(C) two members shall be appointed by the Committee on Energy and Commerce in the House of Representatives, with one member selected by the Chair and the other selected by the Ranking Member;

(D) two members shall be appointed by the Committee on Homeland Security and Government Affairs in the Senate, with one member selected by the Chair and the other selected by the Ranking Member;

(E) two members shall be appointed by the Committee on Foreign Relations in the Senate, with one member selected by the Chair and the other selected by the Ranking Member; and

(F) two members shall be appointed by the Committee on Commerce, Science, and Transportation in the Senate, with one member selected by the Chair and the other selected by the Ranking Member.

(2) QUALIFICATIONS.—

(A) AREAS OF EXPERTISE.—Individuals appointed to the Commission shall be United States persons with experience in such professions as privacy, civil rights, civil liberties, constitutional law, computer science and engineering, digital media and communications, online platform management, cybersecurity, information operations, and national security. The appointment of members to the Commission shall, to the extent possible, be coordinated among nominations to ensure Commission membership represents a variety of expertise in such fields.

(B) PRIVACY, CIVIL RIGHTS, AND CIVIL LIBERTIES.—Not fewer than four individuals appointed to the Commission shall be experts in the fields of privacy, civil rights, or civil liberties, and not fewer than one individual shall be an expert in constitutional law.

(C) NON-GOVERNMENT APPOINTEES.—An individual appointed to the Commission may not be an officer or employee of the Federal Government.

(D) NON-INDUSTRY APPOINTEES.—An individual appointed to the Commission may not be a current officer, employee, contractor, or active or significant shareholder of an entity that owns or operates an online platform.

(3) DEADLINE FOR APPOINTMENT.—Members of the Commission shall be appointed not later than 30 days after the date of the enactment of this Act.

(d) CHAIR.—The Chair shall be chosen from among the members appointed to the Commission on the basis of their qualifications with respect to privacy, civil rights, and civil liberties, through a vote taken by a majority of Commission members or, in the absence of a majority, by a plurality of Commission members.

(e) INITIAL MEETING.—The Commission shall meet and begin operating not later than 30 days after the date of the appointment of its final member.

(f) QUORUM; VACANCIES.—After its initial meeting, the Commission shall meet upon the call of the Chair or a majority of its members. Nine members of the Commission shall constitute a quorum, and members shall have the option to vote by proxy. Any vacancy in the Commission shall not affect its powers, but shall be filled in the same manner in which the original appointment was made.

(g) STUDY AREAS.—The Commission shall, consistent with the purposes specified in subsection (b), analyze existing research that relates to the utilization of online platforms in furtherance of acts of targeted violence, including domestic terrorism and international terrorism, or covert foreign state influence campaigns, identify any areas with respect to which additional research is needed, and study the following:

(1) The extent to which owners or operators of online platforms have been able to respond effectively to attempts to use online platforms in furtherance of acts of targeted violence, including domestic terrorism and international terrorism, or covert foreign state influence campaigns, and what impact, if any, such responses have had on the privacy, civil rights, or civil liberties of users.

(2) The ways, if any, that online platforms' algorithms or other automated decision-making systems may have affected activity on such platforms in furtherance of acts of targeted violence, including domestic terrorism and international terrorism, or covert foreign state influence campaigns.

(3) The extent to which owners or operators of online platforms have transparent, consistent, and equitable policies and procedures to enforce terms of services or codes of conduct, provide notice and an opportunity for redress, or otherwise address violations of platform rules, including a consideration of best practices for improving online platforms' policies and procedures, including the recommendations contained in the Santa Clara Principles on Transparency and Accountability in Content Moderation, as published on February 2, 2018, or successor principles with respect to the extent and impact of content removals and user suspensions and removals, as well as principles related to the notice and appeals of such decisions.

(4) The extent to which owners or operators of online platforms consistently and effectively enforce the policies and procedures described in paragraph (3).

(5) The extent to which owners or operators of online platforms consider the potential use of online platforms in furtherance of targeted violence, including domestic terrorism and international terrorism, or covert foreign state influence campaigns, when evaluating whether to enter into partnerships, advertising agreements, or other business opportunities.

(h) POWERS OF COMMISSION.—

(1) HEARINGS AND EVIDENCE.—For the purpose of carrying out this section, the Commission may—

(A) hold such hearings and sit and act at such times and places, take such testimony, receive such evidence, and administer such oaths, and

(B) require, by subpoena authorized by the majority vote of the Commission, the attendance and testimony of such witnesses and the production of such books, records, correspondence, memoranda, papers, and documents, but only to the extent necessary to achieve the purposes specified in subsection (b).

(2) LIMITATIONS ON SUBPOENA AUTHORITY.—With respect to the subpoena authority granted in paragraph (1)(B), the Commission—

(A) may only issue a subpoena to an owner or operator of an online platform but only to the extent necessary to achieve the purposes specified in subsection (b);

(B) may not, under any circumstances, issue a subpoena for information related to an individual user or group of users;

(C) may not share, disclose, publish, or transmit in any way any information obtained through subpoena to a Federal department or agency, any agency of a State, local, Tribal, or territorial government, or any international body;

(D) may not share, disclose, publish, or transmit in any way any information obtained through subpoena with any individual or organization outside the Commission unless three-fourths of Commission members approve such action and that any such sharing, disclosure, publishing, or transmission be reasonably necessary for the report and to further the Commission's goals; and

(E) shall comply with requirements for the issuance of a subpoena issued by a United States district court under the Federal Rules of Civil Procedure.

(3) PUBLIC MEETINGS AND RELEASE OF PUBLIC VERSIONS OF REPORTS.—

(A) IN GENERAL.—The Commission shall—

(i) hold public hearings and meetings, as appropriate;

(ii) hold closed or classified hearings or meetings, as appropriate;

(iii) provide an opportunity for public comment, including sharing of research and policy analysis, through publication in the Federal Register of a solicitation for public comments during a period to last not fewer than 45 days; and

(iv) release a public version of the report required under subsection (k)(2).

(B) CONDUCT.—Any public hearing, meeting, or reporting of the Commission under this paragraph shall be conducted in a manner consistent with the protection of information provided to or developed for or by the Commission as required by any applicable statute, regulation, or Executive order.

(4) OBLIGATION TO PROTECT PERSONAL INFORMATION.—Whether or not the Commission receives personally identifiable information through the exercise of subpoena authority pursuant to paragraph (1)(B), neither the Commission nor any member of the Commission may publish, disclose, or release such information publicly or to a Federal department or agency, an agency of a State, local, Tribal, or territorial government, any international body, or any other individual or organization outside the Commission.

(5) OBLIGATION TO PROTECT PROPRIETARY INFORMATION.—Whether or not the Commission receives proprietary information, confidential business information, or a trade secret through the exercise of subpoena authority pursuant to paragraph (1)(B), neither the Commission nor any member of the Commission may publish, disclose, or release such information publicly or to a Federal department or agency, an agency of a State, local, Tribal, or territorial government, any international body, or any individual or organization outside the Commission.

(6) COORDINATION WITH AND ASSISTANCE TO THE UNDER SECRETARY FOR SCIENCE AND TECHNOLOGY OF THE DEPARTMENT OF HOMELAND SECURITY.—The Commission may, to the extent practicable—

(A) consult with the Under Secretary for Science and Technology of the Department of Homeland Security on the research conducted in accordance with section 3; and

(B) provide assistance in furtherance of such research, as appropriate.

(7) PERSONALLY IDENTIFIABLE INFORMATION.—In providing testimony or producing books, records, correspondence, memoranda, papers, documents, or any other information or materials to the Commission, either to comply with a subpoena issued under this subsection or for any other purpose, owners or operators of online platforms should review such information or materials for personally identifiable information and should remove such information.

(i) STAFF OF COMMISSION.—The Chair, in consultation with the Vice Chair, and in accordance with rules agreed upon by the Commission, may appoint and fix the compensation of a staff director and such other personnel as may be necessary to enable the Commission to carry out its functions, without regard to the provisions of title 5, United States Code, governing appointments in the competitive service, and without regard to the provisions of chapter 51 and subchapter III of chapter 53 of such title relating to classification and General Schedule pay rates, except that no rate of pay fixed under this subsection may exceed the equivalent of that payable for a position at level V of the Executive Schedule under section 5316 of title 5, United States Code.

(j) SECURITY CLEARANCES FOR COMMISSION MEMBERS AND STAFF.—The heads of appropriate Federal departments and agencies shall cooperate with the Commission in expeditiously providing to Commission members and staff appropriate security clearances to the extent practicable pursuant to existing procedures and requirements, including temporary security clearances, as appropriate. No person may be provided access to classified information under this section without the appropriate security clearance.

(k) REPORTS OF COMMISSION; TERMINATION.—

(1) INTERIM REPORTS.—Not later than one year after the first meeting of the Commission, the Chair shall report to Congress on the activities of the Commission and share interim findings, as have been agreed to by a majority of Commission members.

(2) FINAL REPORT.—Not later than two years after the first meeting of the Commission, the Chair shall submit to the President and Congress a report that contains any findings and recommendations agreed to by a majority of Commission members to address the areas of study under subsection (g), including relating to the following:

(A) Policy mechanisms that would address the Commission's findings in a manner that promotes free speech and innovation on the internet, preserves individual privacy, civil rights, and civil liberties, and upholds the principles of the Constitution.

(B) Policies and procedures that owners or operators of online platforms could implement to address such areas of study that preserve the individual privacy, civil rights, and civil liberties of online platform users.

(C) Mechanisms to improve transparency and accountability related to the matters described in subsection (g), including any best practices identified pursuant to paragraph (3) of such subsection.

(D) Areas with respect to which additional research is required, informed by the evaluation of prior research, as required under subsection (g).

(E) Other matters identified by the majority of Commission members.

(3) TERMINATION.—The Commission shall terminate on the date that is 90 days after the date on which the final report under paragraph (2) is submitted.

(l) ACTION PLAN.—Not later than 180 days after submission of the final report of the Commission pursuant to paragraph (2) of subsection (k), the Secretary of Homeland Security shall issue an action plan in response to findings and recommendations under subparagraph (D) of such paragraph.

(m) PAPERWORK REDUCTION ACT EXEMPTION.—Subchapter I of chapter 35 of title 44, United States Code, shall not apply to this section.

(n) RULE OF CONSTRUCTION.—Nothing in this section may be construed to confer any authority, including law enforcement authority, beyond that which is authorized under existing law.

SEC. 3. RESEARCH.

(a) IN GENERAL.—The Under Secretary for Science and Technology of the Department of Homeland Security shall—

(1) analyze existing research regarding previous acts of targeted violence, including domestic terrorism or international terrorism;

(2) carry out research to better understand whether any connection exists between the use of online platforms, particularly platforms used for social media and social networking, and targeted violence, including domestic terrorism and international terrorism, that takes into consideration how the organization, structure, and presentation of information on an online platform contributes, or does not contribute, to acts of targeted violence, including domestic terrorism or international terrorism; and

(3) develop voluntary approaches that could be adopted by owners and operators of online platforms to address research findings under paragraph (2), while preserving the individual privacy, civil rights, and civil liberties of users and innovation on online platforms.

(b) PARTNERSHIP.—In carrying out this section, the Under Secretary for Science and Technology of the Department of Homeland Security shall, to the extent practicable, coordinate with the National Commission on Online Platforms and Homeland Security under section 2, as well as academic institutions, non-profit organizations, the private sector, and Federal, State, local, and Tribal partners, as appropriate.

(c) REPORT.—Not later than one year after the date of the enactment of this section, the Under Secretary for Science and Technology of the Department of Homeland Security shall submit to Congress a report related to the research and development required under subsection (a).

(d) PAPERWORK REDUCTION ACT EXEMPTION.—Subchapter I of chapter 35 of title 44, United States Code, shall not apply to this section.

SEC. 4. DEFINITIONS.

In this Act:

(1) COVERT FOREIGN STATE INFLUENCE CAMPAIGNS.—The term "covert foreign state influence campaigns" means the coordinated and covert application of state diplomatic, informational, military, economic, business, corruption, edu-

cational, or other capability that was carried out by a foreign state actor to the United States to affect elections in the United States.

(2) DOMESTIC TERRORISM.—The term "domestic terrorism" has the meaning given such term in section 2331 of title 18, United States Code.

(3) INTERNATIONAL TERRORISM.—The term "international terrorism" has the meaning given such term in section 2331 of title 18, United States Code.

(4) ONLINE PLATFORM.—

(A) IN GENERAL.—The term "online platform" means internet-based information services consisting of the storage and processing of information by and at the request of a content provider and the dissemination of such content to third parties.

(B) EXCLUSIONS.—Such term does not include the following:

(i) Platforms the primary purpose of which is to produce journalistic or editorial content (not including editorial decisions by online platforms to rank and organize third party content).

(ii) Applications and functionalities that enable private communications, such as email, direct messages, and end-to-end encrypted communication services.

(iii) Online service providers at layers of the internet infrastructure other than the application layer, and cloud IT infrastructure service providers.

(5) PERSONALLY IDENTIFIABLE INFORMATION.—The term "personally identifiable information" means any information about an individual elicited, collected, stored, or maintained by an agency or owner or operator of an online platform, including the following:

(A) Any information that can be used to distinguish or trace the identity of an individual, such as a name, a social security number, a date and place of birth, a mother's maiden name, phone number or biometric records.

(B) Any other information that is linked or linkable to an individual, such as medical, educational, financial, or employment information.

(6) TARGETED VIOLENCE.—The term "targeted violence" means an incident of violence in which an attacker selected a particular target in order to inflict mass injury or death as part of an act of domestic terrorism or international terrorism or with no discernable political or ideological motivation beyond mass injury or death. Acts of targeted violence include the August 5, 2012, mass shooting at a Sikh temple in Oak Creek, Wisconsin, the June 12, 2016, nightclub mass shooting in Orlando, Florida, the October 1, 2017, attack on concertgoers at a music festival in Las Vegas, Nevada, the October 27, 2018, attack at a synagogue in Pittsburgh, Pennsylvania, and the August 3, 2019, mass shooting at a store in El Paso, Texas.

PURPOSE AND SUMMARY

H.R. 4782, the "National Commission on Online Platforms and Homeland Security Act," would create a bipartisan, 12-member Commission comprised of non-government experts to study the ways, if any, that online platforms, including platforms used for social media and social networking, have been utilized in furtherance of acts of targeted violence, including domestic and international terrorism, as well as covert foreign influence campaigns. The Commission would examine the implications of such use, if any, on free speech, privacy, civil rights and civil liberties, as well as actions taken by platform owners and operators in response to such utilization. The Commission would be tasked with developing recommendations for how online platforms could address such utilization in ways that promote transparency, free speech and innovation on the internet, preserve individual privacy, civil rights, and civil liberties, and uphold the principles of the U.S. Constitution in accordance with relevant statutes, and take into account current or anticipated trends and technological developments, such as advancements in artificial intelligence.

Additionally, H.R. 4782 would direct the Under Secretary for Science and Technology (S&T) of the Department of Homeland Security (DHS) to research whether any connection exists between

the use of online platforms and the tendency of an individual to commit acts of targeted violence, including acts of domestic and international terrorism.

BACKGROUND AND NEED FOR LEGISLATION

Terrorist groups at home and abroad have long made use of the internet to spread their ideologies globally.[1] Since 2013, the Islamic State of Iraq and Syria (ISIS) has used social media to inspire and recruit members across the world, producing relatively polished videos displaying shocking acts of brutality and violence designed to go viral and build the notoriety of the group.[2] Similarly, domestic extremist groups such as white supremacists and anti-government extremists have made use of online platforms to spread their messages and connect with like-minded individuals.

At the same time, the modern information environment has evolved rapidly over the past few years. Mainstream social media platforms have made amplification of content easier while smaller platforms like 8chan and Gab have enabled fringe perspectives to cluster into self-reinforcing "echo chambers,"[3] then gather and communicate privately using encrypted messaging apps like WhatsApp and Telegram.[4] Websites like Stormfront—once labeled the "murder capital of the Internet"[5] by the South Poverty Law Center—has declined in influence[6] as extremists have migrated to websites like the Daily Stormer, 4chan, 8chan, and Gab, which claim to not moderate speech.[7] Meanwhile, terrorists and extremist groups continue to take advantage of mainstream platforms like YouTube and Facebook Live to broadcast to larger audiences.[8]

Hostile foreign governments have also demonstrated an ability to use online platforms as a tool to carry out covert influence campaigns designed to sow political discord, foster societal polarization, and interfere in elections around the world, including the United States.[9] During the 2016 U.S. Presidential election, Russian military and intelligence agencies, working through proxy groups like the Internet Research Agency (IRA), "sought to influence the 2016 U.S. presidential election by harming Hillary Clinton's chances of success and supporting Donald Trump at the direction of the Krem-

---

[1] Antonia Ward, *ISIS's Use of Social Media Still Poses a Threat to Stability in the Middle East and Africa*, RAND, Dec. 11, 2018, https://www.rand.org/blog/2018/12/isiss-use-of-social-media-still-poses-a-threat-to-stability.html.

[2] *Id.*

[3] Anti-Defamation League Center on Extremism and Network Contagion Research Institute, *Gab and 8chan: Home to Terrorist Plots Hiding in Plain Sight*, Apr. 2019, https://www.adl.org/resources/reports/gab-and-8chan-home-to-terrorist-plots-hiding-in-plain-sight.

[4] Audrey Alexander, William Braniff, *Marginalizing Violent Extremism Online*, LAWFARE, Jan. 21, 2018, https://www.lawfareblog.com/marginalizing-violent-extremism-online.

[5] Alex Hern, *Stormfront: 'murder capital of Internet' pulled offline after civil rights action*, THE GUARDIAN, Aug. 29, 2017, https://www.theguardian.com/technology/2017/aug/29/stormfront-neo-nazi-hate-site-murder-internet-pulled-offline-web-com-civil-rights-action.

[6] Kelly Weill, *Stormfront, the Internet's Oldest White Supremacist Website, Says It's Going Broke*, DAILY BEAST, Apr. 10, 2018, https://www.thedailybeast.com/stormfront-the-internets-oldest-white-supremacist-site-says-its-going-broke.

[7] Adi Robertson, *Questions about policing online hate are much bigger than Facebook and YouTube*, THE VERGE, Mar. 15, 2019, https://www.theverge.com/2019/3/15/18267638/new-zealand-christchurch-mass-shooting-online-hate-facebook-youtube.

[8] Emma Gray Ellis, *The Alt-Right are Savvy Internet Users. Stop Letting Them Surprise You*, WIRED, Sept. 19, 2018, https://www.wired.com/story/alt-right-youtube-savvy-data-and-society/.

[9] Office of the Director of National Intelligence, *Assessing Russian Activities and Intentions in Recent U.S. Elections*, ICA 2017–01D (Jan. 6, 2017), https://www.dni.gov/files/documents/ICA_2017_01.pdf.

lin." [10] To do so, the Russian government executed a sophisticated, years-long influence operation using Facebook and other social media platforms to propagate misinformation [11] through inflammatory advertisements and viral content.[12] Most often, this targeted misinformation preyed upon "hot-button, societal divisions in the United States . . . in order to stoke anger, provoke outrage and protest, push Americans further away from one another, and foment distrust in government institutions." [13] Other countries, such as Iran, have also executed misinformation campaigns aimed at influencing public opinion and spreading disinformation.[14]

While Facebook was perhaps the most visible platform utilized during the 2016 Russian influence campaign, it was hardly alone. On Twitter, "junk news" and conspiracy theories flooded users' feeds, particularly in swing states,[15] and YouTube's recommendation algorithms led users toward increasingly extreme video content,[16] with users watching more than 3 billion YouTube-recommended election videos in the lead up to the 2016 election.[17] The Russian government's influence campaign has been documented extensively in indictments brought by the Justice Department and in Special Counsel Robert Mueller's 2019 *Report on the Investigation Into Russian Interference in the 2016 Presidential Election*.[18]

Although public attention has generally focused on the role of social media platforms in making content available to a wide audience, recent reporting suggests that these platforms' algorithms, using features such as "recommendations," may be actively pushing users toward increasingly extreme content [19] tailored to specific users based on, for instance, their past activity on the platform.[20] In May 2019, the Associated Press reported that Facebook's algorithms had actually generated automated terrorist content, for in-

---

[10] Senate Select Committee on Intelligence, *Russian Active Measures Campaigns and Interference in the 2016 U.S. Election Volume I1: Russia's Use of Social Media With Additional Views* (Oct. 2019), https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf.

[11] Here, the term "misinformation" refers to both intentionally and unintentionally misleading content. Sometimes, "disinformation" is used to clarify that the content is intentionally misleading.

[12] Sheera Frenkel and Katie Benner, *To Stir Discord in 2016, Russians Turned Most Often to Facebook*, New York Times, Feb. 17, 2018, https://www.nytimes.com/2018/02/17/technology/indictment-russian-tech-facebook.html.

[13] Senate Select Committee on Intelligence, *Russian Active Measures Campaigns and Interference in the 2016 U.S. Election Volume I1*, at 6.

[14] Jack Stubbs & Christopher Bing, *Exclusive: Iran-based political influence operation—bigger, persistent, global*, REUTERS (Aug 28, 2018), https://www.reuters.com/article/us-usa-iran-facebook-exclusive/exclusive-iran-based-political-influence-operation-bigger-persistent-global-idUSKCN1LD2R9.

[15] Tony Romm and Rani Molla, *Junk news and Russian misinformation flooded Twitter during the 2016 election*, Vox, Sept. 28, 2017, https://www.vox.com/2017/9/28/16378186/twitter-fake-news-misinformation-russia-oxford-swing-states.

[16] Paul Lewis, *'Fiction is outperforming reality': how YouTube's algorithm distorts truth*, The Guardian, Feb. 2, 2018, https://www.theguardian.com/technology/2018/feb/02/how-youtubes-algorithm-distorts-truth.

[17] *Id.*

[18] Special Counsel Robert S. Mueller, III, *Report on the Investigation Into Russian Interference in the 2016 Presidential Election*, U.S. Department of Justice, Mar. 2019, https://www.justice.gov/storage/report.pdf.

[19] Kevin Roose, *The Making of a YouTube Radical*, NEW YORK TIMES, June 8, 2019, https://www.nytimes.com/interactive/2019/06/08/technology/youtube-radical.html; *see also* Zeynep Tufekci, *Opinion: YouTube, the Great Radicalizer*, NEW YORK TIMES, Mar. 10, 2018, https://www.nytimes.com/2018/03/10/opinion/sunday/youtube-politics-radical.html ("Given its billion or so users, YouTube may be one of the most powerful radicalizing instruments of the 21st century.")

[20] Craig Silverman, Jane Lytvynenko, and Lam Thuy Vo, *How Facebook Groups Are Being Exploited To Spread Misinformation, Plan Harassment, And Radicalize People*, BUZZFEED NEWS, Mar. 19, 2018, https://www.buzzfeednews.com/article/craigsilverman/how-facebook-groups-are-being-exploited-to-spread.

stance by turning propaganda videos by jihadist terrorist groups into an "anniversary" video celebrating one year of the users' content.[21] In another case, the National Whistleblower Center found that Facebook automatically generated a page for the Syrian terrorist group Hayat Tahrir al-Sham.[22] The site was still live as of June 24, 2019, nearly two months after the initial report, with nearly 4,500 "likes."

As a whole, social media companies and other online platforms have been slow to respond to the proliferation of terrorist content and the spread of disinformation on their sites. Recent terrorist attacks in Christchurch, New Zealand,[23] El Paso, Texas,[24] Halle, Germany,[25] and elsewhere—have raised serious questions about the use of online platforms by terrorists and other bad actors wanting to amplify and share violent terrorist content. At the same time, some of the solutions that have been proposed to address these problems may have the unintended consequence of restricting free speech, stifling innovation, or targeting already-vulnerable groups in the name of rooting out bad actors.

The problem of terrorist content on online platforms is, in some ways, distinct from the use of these platforms to carry out foreign influence campaigns; however, there are also many commonalities. At the core of each is a focus on divisive, polarizing content and a tendency to prey on those most marginalized in modern society. The solution to the proliferation of terrorist content on online platforms will necessarily involve the owners and operators of online platforms developing better strategies to manage platform features and content in ways that are transparent, equitable, consistent, and enforceable.

Studies have shown that mass killings inspire copycats,[26] raising concerns that terrorist content that goes viral on social media platforms may inspire the next act of mass violence. In addition, ideologically-motivated mass killings may inspire retaliatory attacks.[27] This is an area where continued study is needed that to enhance our understanding of what connection, if any, exists between the

---

[21] Desmond Butler and Barbara Ortutay, *Facebook auto-generates videos celebrating extremist images*, ASSOCIATED PRESS, May 9, 2019, https://www.apnews.com/f97c24dab4f34bd0b48b36f2988952a4.

[22] *Radical Connections: How Facebook Helps Terrorists and Hate Groups Network on its Website*, NATIONAL WHISTLEBLOWER CENTER, Apr. 29, 2019, https://www.whistleblowers.org/wp-content/uploads/2019/05/Facebook-SEC-Petition-2019.pdf.

[23] Charlotte Graham-McLay, *Death Toll in New Zealand Mosque Shootings Rises to 51*, NEW YORK TIMES, May 2, 2019, https://www.nytimes.com/2019/05/02/world/asia/new-zealand-attack-death-toll.html.

[24] Robert Moore and Mark Berman, *Officials call El Paso shooting a domestic terrorism case, weigh hate crime charges*, WASHINGTON POST, Aug. 4, 2019, https://www.washingtonpost.com/nation/2019/08/04/investigators-search-answers-after-gunman-kills-el-paso/.

[25] Luisa Beck and Rick Noack, *Synagogue attacker hoped to inspire further anti-Semitic attacks, German authorities say*, WASHINGTON POST, Oct. 10, 2019, https://www.washingtonpost.com/world/europe/after-deadly-attack-outside-halle-synagogue-jewish-community-worries-about-safety-in-germany/2019/10/10/434b2ce8-eae5-11e9-a329-7378fbfa1b63_story.html.

[26] *See, e.g.*, Maggie Fox, *Mass killings inspire copycats, study finds*, NBC NEWS, July 2, 2015, https://www.nbcnews.com/health/health-news/yes-mass-killings-inspire-copycats-study-finds-n386141; *Number of mass shootings in US has risen sharply, FBI report says,* THE GUARDIAN, Sep. 25, 2014, https://www.theguardian.com/world/2014/sep/25/us-mass-shootings-risen-sharply-fbi-report ("'The copycat phenomenon is real,' said Andre Simons of the FBI's Behavioral Analysis Unit. 'As more and more notable and tragic events occur, we think we're seeing more compromised, marginalized individuals who are seeking inspiration from those past attacks.'")

[27] *See, e.g,. Joint Intelligence Bulletin: Attacks on Mosques in Christchurch, New Zealand, May Inspire Supporters of Violent Ideologies*, DEPT. OF HOMELAND SECURITY, FEDERAL BUREAU OF INVESTIGATION, NATIONAL COUNTERTERRORISM CENTER, Mar. 15, 2019 (attached).

use of online platforms and the perpetration of targeted acts of violence, and also to inform future policymaking.

Although the spread of online misinformation is well-established, there is a dearth of scientific and academic research necessary to understand it. While the number of reports of such utilization has grown, the research to understand what, if any, correlation exists between the use of online platforms and the spread of disinformation or perpetration of acts of targeted violence is still fairly nascent. There may not be a connection at all or if there is, it may not align with common understanding or suppositions of the public, law enforcement, and policymakers.

The Commission, established under H.R. 4782, would be chaired by an expert in privacy, civil rights, or civil liberties and its membership will include individuals with expertise in those areas, as well as computer science and engineering, digital media and communications, online platform management, cybersecurity, information operations, and national security. The Commission will be charged with studying:

- How effectively platform owners and operators have been able to respond to the use of their platforms in furtherance of targeted violence, including domestic and international terrorism, or covert foreign state influence campaigns.
- The ways, if any, that algorithms and other automated decision-making systems may impact privacy, civil rights, and civil liberties, or affect online activity in furtherance of targeted violence, including domestic and international terrorism, or covert foreign state influence campaigns.
- The extent to which platforms have transparent, consistent, and equitable policies to enforce terms of service or codes of conduct, provide notice and opportunity for redress, or otherwise address violations of platform rules consistent with the *Santa Clara Principles on Transparency and Accountability in Content Moderation*, and other best practices.
- The extent to which online platforms consistently and effectively enforce their platform rules.
- Whether owners and operators of online platforms consider the potential for platforms to be used in furtherance of targeted violence, including domestic and international terrorism, or covert foreign state influence campaigns when evaluating potential partnerships, advertising agreements, or business opportunities.

The Commission is granted limited subpoena authority to compel operational information from online platforms—but cannot compel information related to an individual user or group of users—to inform a report, to be published two years after the first Commission meeting, that includes recommendations on: (1) policy mechanisms to address findings in a manner that promotes free speech, privacy and civil liberties, and other Constitutional principles; (2) voluntary policies and procedures that platforms could implement to address Commission findings in accordance with such Constitutional principles; (3) voluntary mechanisms to improve transparency and accountability; and (4) areas where additional research is required.

This legislation would also require the Secretary of Homeland Security to issue an action plan in response to the Commission's findings regarding areas where additional research is required.

HEARINGS

For the purposes of section 103(i) of H. Res 6. of the 116th Congress, the following hearings were used to develop H.R. 4782:

- On June 25, 2019, the Committee held a hearing entitled "Artificial Intelligence and Counterterrorism: Possibilities And Limitations." The Committee received testimony from Mr. Ben Buchanan, Assistant Teaching Professor, Georgetown University; Senior Faculty Fellow, Center for Security and Emerging Technology; Mr. Alex Stamos, Adjunct Professor, Freeman Spogli Institute; Program Director, Stanford Internet Observatory; and Mr. Julian Sanchez, Senior Fellow, Cato Institute.
- On June 26, 2019, the Committee held a hearing entitled "Examining Social Media Companies" Efforts to Counter Online Terror Content and Misinformation." The Committee received testimony from Ms. Monika Bickert, Head of Global Policy Management, Facebook; Mr. Nick Pickles, Global Senior Strategist, Public Policy, Twitter; Mr. Derek Slater, Global Director of Information Policy, Google; and Ms. Nadine Strossen, John Marshall Harlan II Professor of Law, New York Law School.

COMMITTEE CONSIDERATION

The Committee met on October 23, 2019, with a quorum being present, to consider H.R. 4782 and ordered the measure to be reported to the House with a favorable recommendation, with an amendment, by unanimous consent.

The following amendment was offered and agreed to by unanimous consent:

An amendment offered by Mr. Thompson.

Page 4, line 24, insert "constitutional law" after "civil liberties,".

Page 5, line 12, insert ", and not fewer than one individual shall be an expert in constitutional law".

Page 7, strike lines 9 through 16, and insert the following:

> (2) The ways, if any, that online platforms' algorithms or other automated decision-making systems may have affected activity on such platforms in furtherance of acts of targeted violence, including domestic terrorism and international terrorism, or covert foreign state influence campaigns.

Page 9, beginning line 5, strike "as the Commission may determine advisable" and insert "but only to the extent necessary to achieve the purposes specified in subsection (b)".

Page 9, line 11, insert "but only to the extent necessary to achieve the purposes specified in subsection (b)" before the semicolon.

Page 10, line 1, strike "and that".

Page 10, line 3, insert "for the report and" before "to further".

Page 11, strike line 19 through page 12, line 2, and insert the following:

(5) OBLIGATION TO PROTECT PROPRIETARY INFORMATION.—Whether or not the Commission receives proprietary information, confidential business information, or a trade secret through the exercise of subpoena authority pursuant to paragraph (1)(B), neither the Commission nor any member of the Commission may publish, disclose, or release such information publicly or to a Federal department or agency, an agency of a State, local, Tribal, or territorial government, any international body, or any individual or organization outside the Commission.

Page 16, line 22, strike "users.." and insert "users and innovation on online platforms.".

Page 17, line 20, strike "by foreign state actors'" and insert "that was carried out by a foreign state actor".

Page 18, line 14, strike "that offer" and insert "the primary purpose of which is to produce".

Page 18, line 20, insert "end-to-end" before "encrypted".

Page 19, line 11, insert "phone number," before "or biometric".

Page 19, strike line 15 and all that follows through page 20, line 2, and insert the following:

(6) TARGETED VIOLENCE.—The term "targeted violence" means an incident of violence in which an attacker selected a particular target in order to inflict mass injury or death as part of an act of domestic terrorism or international terrorism or with no discernable political or ideological motivation beyond mass injury or death. Acts of targeted violence include the August 5, 2012, mass shooting at a Sikh temple in Oak Creek, Wisconsin, the June 12, 2016, nightclub mass shooting in Orlando, Florida, the October 1, 2017, attack on concert-goers at a music festival in Las Vegas, Nevada, the October 27, 2018, attack at a synagogue in Pittsburgh, Pennsylvania, and the August 3, 2019, mass shooting at a store in El Paso, Texas.

COMMITTEE VOTES

Clause 3(b) of rule XIII of the Rules of the House of Representatives requires the Committee to list the recorded votes on the motion to report legislation and amendments thereto.

No recorded votes were requested during consideration of H.R. 4782.

COMMITTEE OVERSIGHT FINDINGS

In compliance with clause 3(c)(1) of rule XIII of the Rules of the House of Representatives, the Committee advises that the findings and recommendations of the Committee, based on oversight activities under clause 2(b)(1) of rule X of the Rules of the House of Representatives, are incorporated in the descriptive portions of this report.

CONGRESSIONAL BUDGET OFFICE ESTIMATE, NEW BUDGET AUTHORITY, ENTITLEMENT AUTHORITY, AND TAX EXPENDITURES

With respect to the requirements of clause 3(c)(2) of rule XIII of the Rules of the House of Representatives and section 308(a) of the Congressional Budget Act of 1974 and with respect to requirements

of clause (3)(c)(3) of rule XIII of the Rules of the House of Representatives and section 402 of the Congressional Budget Act of 1974, the Committee adopts as its own the cost estimate prepared by the Director of the Congressional Budget Office.

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, October 31, 2019.

Hon. BENNIE G. THOMPSON,
Chairman, Committee on Homeland Security,
House of Representatives, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 4782, the National Commission on Online Platforms and Homeland Security Act.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Aldo Prosperi.

Sincerely,

PHILLIP L. SWAGEL,
Director.

Enclosure.

H.R. 4782, National Commission on Online Platforms and Homeland Security Act

As ordered reported by the House Committee on Homeland Security on October 23, 2019

By Fiscal Year, Millions of Dollars	2020	2020-2024	2020-2029
Direct Spending (Outlays)	0	0	0
Revenues	0	0	0
Increase or Decrease (-) in the Deficit	0	0	0
Spending Subject to Appropriation (Outlays)	3	5	5

Statutory pay-as-you-go procedures apply?	No	**Mandate Effects**	
Increases on-budget deficits in any of the four consecutive 10-year periods beginning in 2030?	No	Contains intergovernmental mandate?	No
		Contains private-sector mandate?	No

H.R. 4782 would require the Department of Homeland Security (DHS) to research how online platforms may be used to facilitate acts of terrorism. On the basis of information from DHS regarding the costs of similar research efforts, CBO estimates implementing that provision would cost $4 million.

The bill also would establish a national commission to study how entities have used social media and other online platforms to threaten U.S. national security. The commission would be required to provide recommendations on ways to mitigate the effects of online terrorist content and electoral-disinformation campaigns. The commission would terminate after two years. Using information about the costs of similar commissions, CBO estimates that staff salaries, security clearance costs, and other expenses would be $1 million.

In total, CBO estimates that implementing the bill would increase spending by $5 million over the 2020–2024 period; such spending would be subject to the availability of appropriations.

The CBO staff contact for this estimate is Aldo Prosperi. The estimate was reviewed by Leo Lex, Deputy Assistant Director for Budget Analysis.

FEDERAL MANDATES STATEMENT

The Committee adopts as its own the estimate of Federal mandates prepared by the Director of the Congressional Budget Office pursuant to section 423 of the Unfunded Mandates Reform Act.

DUPLICATIVE FEDERAL PROGRAMS

Pursuant to clause 3(c) of rule XIII, the Committee finds that H.R. 4782 does not contain any provision that establishes or reauthorizes a program known to be duplicative of another Federal program.

PERFORMANCE GOALS AND OBJECTIVES

Pursuant to clause 3(c)(4) of rule XIII of the Rules of the House of Representatives, the objective of H.R. 4782 is to establish a National Commission on Online Platforms and Homeland Security, comprised of 12 members appointed on a bipartisan basis by Chairs and Ranking Members of relevant Committees in the House of Representatives and the Senate. The Commission would identify, examine, and report on the ways, if any, that online platforms have been utilized in furtherance of acts of targeted violence, including domestic and international terrorism, or covert foreign state influence campaigns, as well as various actions taken in response to such utilization by owners and operators of online platforms and implications for the privacy, civil rights, and civil liberties of individuals. The Commission would be tasked with producing an interim and final report within one and two years, respectively, of its first meeting. The Committee expects that these reports would identify actionable policy mechanisms to address the Commission's findings, policies and procedures that platform owners and operators could adopt on their platforms to improve transparency and accountability and areas where additional research is needed. For all findings and recommendations, the Committee expects that the Commission will seek to promote Constitutional principles, including free speech, individual privacy, civil rights and civil liberties, while at the same time protecting innovation on the internet.

ADVISORY ON EARMARKS

In compliance with rule XXI of the Rules of the House of Representatives, this bill, as reported, contains no congressional earmarks, limited tax benefits, or limited tariff benefits as defined in clause 9(d), 9(e), or 9(f) of the Rule XXI.

SECTION-BY-SECTION ANALYSIS OF THE LEGISLATION

Section 1. Short title

This section states that the Act may be cited as the "National Commission on Online Platforms and Homeland Security Act."

Sec 2. National Commission on Online Platforms and Homeland Security

This section establishes a National Commission on Online Platforms and Homeland Security, for the purposes of identifying, examining, and reporting on the ways, if any, that: (1) online platforms have been utilized in furtherance of acts of targeted violence, including domestic terrorism and international terrorism, or covert foreign state influence campaigns; and (2) free speech, privacy, civil rights and civil liberties are impacted by such utilization on online platforms, as well as policies, procedures, or activities undertaken by owners and operators of online platforms to prevent or limit such utilization. The Commission is also tasked with developing recommendations for how online platforms could address such utilization in ways that are transparent and accountable, promote free speech and innovation on the internet, preserve individual privacy, civil rights, and civil liberties, and uphold the principles of the Constitution in accordance with relevant statutes, and taking into account current or anticipated trends and technological developments, such as advancements in artificial intelligence.

With this section, the Committee intends to set forth a scope of study that is broad enough to encompass new and emerging issues that platforms may confront in the coming years, while limiting the focus of investigation to past instances of targeted violence and foreign influence. The reason for this framing is that the Commission should not become a vessel for investigating contemporaneous or potential future acts of terrorism or disinformation. The Committee expects the Commission to investigate the actions and practices of online platforms, not individual users or groups of users.

Commission Membership

The Commission shall be composed of 12 members appointed by the Chair or Ranking Member of each of the following Committees: the Committee on Homeland Security, the Committee on Foreign Affairs, and the Committee on Energy and Commerce in the House of Representatives, as well as the Committee on Homeland Security and Governmental Affairs, the Committee on Foreign Relations, and the Committee on Commerce, Science, and Transportation in the Senate. Each Chair and each Ranking Member will be allotted one appointment.

Individuals appointed to the Commission shall be United States persons with experience in such professions as privacy, civil rights, civil liberties, computer science and engineering, digital media and communications, online platform management, cybersecurity, information operations, and national security. The appointment of members to the Commission shall, to the extent possible, be coordinated among nominations to ensure Commission membership represents a variety of expertise in such fields.

The Committee intends that the Commission will be led by and comprised of individuals with ample experience in privacy, civil rights, and civil liberties. Therefore, this section provides that at least four individuals appointed to the Commission shall be experts in those fields, and the Chair shall be chosen from among those members.

Because of the sensitive nature of its areas of study, it is important that Commissioners be objective, impartial, and not be per-

ceived as an entrenched arm of the Federal government. Therefore, no Federal officers or employees may serve on the Commission, nor may any current officer, employee, contractor, or active or significant shareholder of an entity that owns or operates an online platform.

Study Areas

The Commission shall analyze existing research that relates to the utilization of online platforms in furtherance of acts of targeted violence, including domestic terrorism and international terrorism, or covert foreign state influence campaigns, identify any areas with respect to which additional research is needed, and study the following:

(1) The extent to which owners or operators of online platforms have been able to respond effectively to attempts to use online platforms in furtherance of acts of targeted violence, including domestic and international terrorism, or covert foreign state influence campaigns, and what impact, if any, such responses have had on the privacy, civil rights, or civil liberties of users.

(2) The ways, if any, that online platforms' algorithms or other automated decision-making systems may have affected activity on such platforms in furtherance of acts of targeted violence, including domestic and international terrorism, or covert foreign state influence campaigns.

(3) The extent to which owners or operators of online platforms have transparent, consistent, and equitable policies and procedures to enforce terms of services or codes of conduct, provide notice and an opportunity for redress, or otherwise address violations of platform rules, including a consideration of best practices for improving online platforms' policies and procedures and the recommendations contained in the *Santa Clara Principles on Transparency and Accountability in Content Moderation*, as published on February 2, 2018, or successor principles with respect to the extent and impact of content removals and user suspensions and removals, as well as principles related to the notice and appeals of such decisions.

(4) The extent to which owners or operators of online platforms consistently and effectively enforce the policies and procedures described in paragraph (3).

(5) The extent to which owners or operators of online platforms consider the potential use of online platforms in furtherance of targeted violence, including domestic terrorism and international terrorism, or covert foreign state influence campaigns, when evaluating whether to enter into partnerships, advertising agreements, or other business opportunities.

The Committee intends that, for each area of study listed in this section, the Commission will be prioritize the promotion of free speech and innovation on the internet, the preservation of individual privacy, civil rights and civil liberties, and the need to uphold the principles of the Constitution.

Powers of Commission

This section authorizes the Commission to hold such hearings and sit and act at such times and places, take such testimony, re-

ceive such evidence, and administer such oaths as necessary or advisable in carrying out this section.

Further, the Commission may require, by subpoena authorized by the majority vote of the Commission, the attendance and testimony of such witnesses and the production of such books, records, correspondence, memoranda, papers, and documents, as the Commission may determine advisable. However, the Committee also intends that the Commission should use its subpoena authority for the purposes of investigating the policies and practices of online platforms, as opposed to any individual user or group of users. Therefore, the Commission may only issue a subpoena to a platform owner or operator, and may not, under any circumstances, issue a subpoena for information related to an individual user or group of users.

Moreover, the Commission may not share, disclose, publish, or transmit any information obtained through subpoena to a Federal agency, State, local, Tribal, or territorial government, or any international body. The Commission is also prohibited from sharing, disclosing, publishing, or transmitting information obtained through subpoena with any individual or organization outside the Commission unless three-fourths of Commission members approve such action. Any such sharing, disclosure, publishing, or transmission should be reasonably necessary to further the Commission's goals.

In providing testimony or producing information to the Commission, either to comply with a subpoena or for any other purpose, owners and operators of online platforms should review such information or materials for personally identifiable information (PII) and remove such information. However, should the Commission nevertheless receive PII, by subpoena or otherwise, neither the Commission nor any member of the Commission may publish, disclose, or release such information publicly or to any Federal agency, State, local, Tribal, or territorial government, international body, or other individual or organization outside the Commission.

In the event that the Commission determines that information received from an owner or operator of an online platform includes confidential business information, a trade secret, or other proprietary information, the Commission shall ensure such information is not published, disclosed, or released to any individual or organization outside the Commission.

The Commission may, to the extent practicable, consult with the DHS Under Secretary for S&T on the research conducted in accordance with section 3, and provide assistance in furtherance of such research, as appropriate.

Not later than one year after the first meeting of the Commission, the Chair shall report to Congress on the activities of the Commission and share interim findings, as have been agreed to by a majority of Commission members. Not later than two years after the first meeting of the Commission, the Chair shall submit to the President and Congress a report that contains any findings and recommendations agreed to by a majority of Commission members to address the required areas of study, including relating to the following:

(A) Policy mechanisms that would address the Commission's findings in a manner that promotes free speech and innovation

on the internet, preserves individual privacy, civil rights, and civil liberties, and upholds the principles of the Constitution.

(B) Policies and procedures that owners or operators of online platforms could implement to address such areas of study that preserve the individual privacy, civil rights, and civil liberties of online platform users.

(C) Mechanisms to improve transparency and accountability related to the matters described in subsection (g), including any best practices identified pursuant to paragraph (3) of such subsection.

(D) Areas with respect to which additional research is required, informed by the evaluation of prior research, as required under subsection (g).

(E) Other matters identified by the majority of Commission members.

The Commission shall terminate 90 days after the date on which the final report is submitted.

Not later than 180 days after submission of the final report of the Commission, the Secretary of Homeland Security is required to issue an action plan in response to the findings and recommendations of the Commission.

Clarifies that nothing in this section may be construed to confer any authority, including law enforcement authority, beyond that which is authorized under existing law and that subchapter I of chapter 35 of title 44, United States Code shall not apply to this section.

Sec 3. Research

This section directs the DHS Under Secretary for S&T to analyze existing research that has been conducted regarding previous acts of targeted violence, including domestic and international terrorism, and conduct new research to better understand whether any connection exists between the use of online platforms, particularly platforms used for social media and social networking, and targeted violence. Such research shall take into consideration how the organization, structure, and presentation of information on online platforms contributes, or does not contribute, to such acts of targeted violence. This section further requires S&T to develop voluntary approaches that platform owners and operators could adopt to address research findings, while preserving the individual privacy, civil rights, and civil liberties of users. S&T shall submit a report with its findings to Congress within one year of the date of enactment.

This section is intended to address concerns about the dearth of academic or scientific research establishing, first and foremost, whether there is a connection between the use of online platforms and the tendency of an individual to commit acts of targeted violence. There is a need for, at a minimum, a catalog or inventory of existing and ongoing research efforts as a starting point to understand comprehensive findings and research gaps.

In carrying out this section, S&T shall, to the extent practicable, coordinate with the National Commission on Online Platforms and Homeland Security, as well as academic institutions, non-profit organizations, the private sector, and Federal, State, local, and Tribal partners, as appropriate.

Further, subchapter I of chapter 35 of title 44, United States Code shall not apply to this section.

Sec 4. Definitions

This section provides definitions for the following terms: "covert foreign state influence campaigns"; "domestic terrorism"; "international terrorism"; "online platform"; "personally identifiable information"; and "targeted violence."

MINORITY VIEWS

On October 23, 2019, the Committee on Homeland Security favorably reported H.R. 4782 as amended with bipartisan support. The legislation establishes a bipartisan commission of nongovernmental individuals, including first amendment experts, to examine and make recommendations regarding terror, extremist and foreign influence content on online platforms.

Social media platforms are entrenched in today's society as forums for communication. These platforms have the ability to bring awareness to humanitarian crisis, share joyful messages, and connect friends and family. However, Republican Members remain concerned about the ability of this content to radicalize individuals to violence, spread hateful ideologies, and mislead the public with false information. Republican Members support H.R. 4782 in order to convene a body of outside experts to examine these challenges, the ongoing work of the platform owners and operators, and vital first amendment protections.

Online platforms were slow to respond to the growth of terror and extremist content on their sites. In the past several years, however, there has been a real effort on behalf of many of the U.S.-based mainstream companies to share information, develop technological tools, and establish rules and policies for content on their sites. For example, on June 26, 2017, Facebook, Twitter, YouTube, and Microsoft announced the creation of the Global Internet Forum to Counter Terrorism (GIFCT) as a voluntary industry-led effort "to substantially disrupt terrorists" ability to promote terrorism, disseminate violent extremist propaganda, and exploit or glorify real-world acts of violence using our platforms."[1] On September 23, 2019, the members of the GIFCT announced that the organization "will become an independent organization led by an Executive Director and supported by dedicated technology, counterterrorism and operations teams."[2] In addition to the GIFCT, the major U.S.-based social media companies have taken independent steps to review content on their platforms. These efforts including hiring additional personnel, expanding programs to allow users to flag extremist content, implementing advanced technology, and promoting counter messaging. While these efforts are to be applauded, there is value in having an outside body conduct a comprehensive review and make additional recommendations for action.

During a Full Committee hearing on June 26, 2019, entitled "Examining Social Media Companies" Efforts to Counter Online Terror Content and Misinformation," Members heard directly from technology platforms, as well as the Republican-invited witness, Pro-

[1] Global Internet Forum to Counter Terrorism, "About our Mission." Accessed June 18, 2019 at https://gifct.org/about/.

[2] Global Internet Forum to Counter Terrorism "Next Steps for GIFCT," September 23, 2019. Accessed February 3, 2020 at https://gifct.org/press/next-steps-gifct/.

fessor Nadine Strossen, who testified about vital First Amendment protections and raised concerns that content moderation is inherently biased. Professor Strossen testified that "[t]he concepts of hate speech, terrorist content and misinformation are all irreducibly vague and broad, therefore having to be enforced according to the subjective discretion of the enforcing authorities. And the discretion has been enforced in ways that both under suppress speech that does pose a serious danger . . . but also suppress very important speech . . . speech that actually counters terrorism and other dangers." [3] She further noted that efforts to remove such content may have the unintended consequence of sending someone to "take refuge in darker corners of the web where it is much harder to engage with them, to use them as sources of information for law enforcement and counterterrorism investigations." [4] Professor Strossen recommended that digital platforms focus on "other approaches that are consistent with free speech and democracy," such as counter narratives and user redirection, as well as "user-empowering technology that would allow us users to make truly informed, voluntary decisions about what we see and what we don't see, and not manipulate us, as has been reported many times, in to increasing rabbit holes and echo chambers, but give us the opportunity to make our own choices and to choose our own communities." [5]

Professor Strossen also addressed concerns related to foreign influence on digital platforms and noted that "[u]ltimately, the only protection that we are going to have in this society against disinformation is from training and education starting at the earliest levels of a child's education in media literacy, because Congress could never protect against misinformation in traditional media unless it meets the very strict standards of defamation that is punishable and fraud that is punishable." [6]

It is vital that the Commission established under H.R. 4782 include members with First Amendment expertise, as well as civil rights and civil liberties. Additionally, the Commission must meet with organizations representing these perspectives as they seek to carry out their work.

Republican edits adopted to the bill ensure that the legislation respects free speech by removing prior text that allowed examination of speech that "potentially posed a threat" to security. Political dissidents off all stripes have been silenced in the name of social stability and security. Republican Members appreciate the removal of this language from draft text.

Additionally, Republican edits curbed the creation of a joint intelligence community and law enforcement task force to examine U.S. citizen speech online. Protecting against terrorism and covert foreign state influence campaigns is important, but more appropriate authorities already exist to combat those threats without breaking down traditional firewalls between domestic law enforcement and our foreign intelligence apparatus. Republican Members appreciate the removal of this language from draft text.

---

[3] Testimony of Ms. Nadine Strossen before the Committee on Homeland Security hearing on "Examining Social Media Companies" Efforts to Counter Online Terror Content and Misinformation," held on June 26, 2019.
[4] Ibid.
[5] Ibid
[6] Ibid.

Committee Republicans also productively engaged with stakeholders and the Majority to more clearly define the term "Online Platform" to protect journalism, private communication and opinion, and non-public internet infrastructure. The rapid convergence of many previously distinct services into large online platforms has greatly complicated legislative efforts to coherently address different types of technology. Republican Members appreciate all feedback received on this issue and recognize that additional work may be needed to accurately address this topic.

Republican Members appreciate the bipartisan way in which this legislation was developed, including several months of negotiations and multiple bipartisan Member and staff meetings with stakeholders.

MIKE ROGERS.

○